DOI: 10.53469/jtpes.2024.04(12).01

Computer Network Security and Preventive Measures in the Era of Big Data

Jun Xiang

Chengdu Jincheng College Chengdu 611731, Sichuan, China

Abstract: ***With the continuous development of networked information technology in China, the incidence of computer network security issues is also increasing. Once a computer encounters a network security issue, it will directly affect people's normal life and production. Therefore, computer users need to have strong awareness of network security management, take effective measures to prevent computer network security issues, and reduce the incidence of computer network security problems.***

Keywords: Computer; Network security; Problem; Preventive measures.

1. OVERVIEW OF COMPUTER NETWORK SECURITY

In the era of big data, computer network security issues are becoming increasingly prominent. With the rapid development of information technology, the Internet has become an important force to promote the progress of human society, but the ensuing network security problems are also emerging in endlessly[1]. Frequent security incidents such as virus outbreaks and hacker attacks pose a serious threat to users' information and property security. These security issues not only affect individuals' daily lives, but may also impact national security and social stability. The computer network security in the era of big data has become a global focus of attention. Many users have insufficient knowledge of computer network security and weak awareness of prevention, making them easy targets for network attacks[2]. For example, randomly clicking on unknown links, downloading files from unknown sources, or performing sensitive operations in insecure network environments[3]. Most computer devices are equipped with operating systems and software that have vulnerabilities that can be exploited by hackers to launch attacks. At the same time, defects in the software development process may also lead to security issues[4]. The diversification of information sources and open sharing channels in computer networks provide convenience for network intruders. They can use these channels to invade systems, steal information, or spread viruses[5].

1.1 Strong confidentiality

In the era of big data, information transmission transcends borders and has no boundaries. The government is no longer the sole owner and authoritative publisher of information[6]. The diversification and decentralization of information control subjects pose unprecedented challenges to confidentiality work. The massive amount of complex and sensitive data hidden within big data itself has become a "big target" for cyber attacks, therefore, high confidentiality is particularly important in the era of big data[7]. Big data technology can correlate and analyze non confidential data, uncover important hidden value information, thereby blurring the boundary between confidential and non confidential, and requiring higher requirements for anti theft and anti leakage measures. The importance of basic data in non-traditional security fields is gradually becoming apparent, and improper sharing, dissemination, and disclosure can pose a huge threat to national security[8]. At the same time, information disclosure and resource sharing have become inevitable requirements, and the confidentiality of some information is gradually weakening[9]. The highly integrated nature of people, machines, and objects has profoundly changed the way state secrets exist, making the channels for leaks more diverse and increasing the difficulty of confidentiality work[10]. Utilize big data analysis technology to enhance the detection and prevention capabilities of unknown threats, and adopt big data based authentication technology to reduce the security risks of authentication attacks[11]. Improve laws and regulations: Establish and improve legislation on network data and personal information security, strengthen big data supervision mechanisms, and ensure that the update speed of security protection measures keeps up with the pace of big data development[12]. Strengthen confidentiality education for personnel involved in sensitive data, enhance confidentiality awareness, ensure strict compliance with confidentiality regulations when handling sensitive data, and prevent information leakage[13][14].

1.2 Faster speed of data information dissemination

The dissemination of data information on the internet is not affected by time and geography, and can expand the scope of information dissemination in the shortest possible time. It is precisely based on the above characteristics that there is a greater need to strengthen effective management of computer network security and improve the security and stability of computer network systems[15][16].

2. THE PROBLEMS FACED BY COMPUTER NETWORK SECURITY

2.1 Invasion of Computer Viruses

Usually, computer viruses lurk within computer programs, and criminals can cause serious impact and damage to computer and network system security by writing virus programs. Once a virus invades, the information and related programs in the computer system are easily maliciously stolen, destroyed, and copied, and in severe cases, can cause serious system crashes. Computer viruses have strong concealment, infectivity, and parasitism, and are usually spread through local area network sharing and network media, making it difficult to completely eliminate them.

2.2 Threats of Computer Network Vulnerabilities

Microsoft software is currently the most widely used computer system by computer users. However, pirated Microsoft software is constantly emerging on the market, posing numerous vulnerabilities to computer networks and posing a great threat to network security. In an open network environment, if users engage in non-standard browsing behavior, it is easy for viruses to enter the computer and attack the internal system, resulting in numerous computer vulnerabilities and threatening the security of the entire network system.

2.3 Violations by Computer Users

The illegal operations of computer users are also an important cause of computer network security issues. According to the survey, the majority of computer users in China have poor awareness of data security, lack professional knowledge of computer operations, and lack understanding of computer security protection theory and technology, resulting in behaviors such as browsing web pages, commenting, liking, and forwarding information at will during computer operations. If a user browses a webpage containing viruses, it will open the door to the invasion of network viruses and cause significant computer network security issues.

2.4 Threats of spyware and spam emails

Computer networks have strong openness, and many data information are interconnected, which creates conditions for illegal personnel to invade. Some illegal individuals may use spam emails to spread network viruses. Computer users may inadvertently authorize the use of these spam emails. Once these viruses are opened, they will invade the entire computer network. At this time, illegal personnel will steal or tamper with important data, and stealing users' personal privacy will have a serious impact on the computer network system.

2.5 Network Hacker Attacks

Network hackers refer to attackers who illegally access and damage users' networks through the internet. Hackers can peek into others' privacy and manipulate or destroy users' information in various ways. Therefore, the uncertainty of hacker motives has a significant impact on users' interests and security. If hackers only pry into users' privacy out of curiosity and do not damage their network systems, although the harm to them is relatively small, it still causes certain harm to users. If hackers have malicious intentions to damage users' network systems, the consequences would be unimaginable. For example, some hackers may attack users' target web pages and content, which can cause network paralysis and prevent users from using them normally, posing a great threat to their own interests; Some hackers have negative emotions, such as malicious attacks and destructive psychology, tampering and destroying important data information in users' computers. In severe cases, it may pose a threat to national defense, military, economic, political and other confidential intelligence, putting national security at the center of public criticism.

2.6 Computer hardware facility failures

Computer hardware configuration failures can also cause corresponding network security issues. If the staff does not regularly maintain and upkeep the computer hardware settings, once some hardware facilities fail, it will interfere with the normal operation of the entire network system, not only reducing the speed of computer operation, but also causing incomplete display of some important information.

3. PREVENTIVE MEASURES FOR COMPUTER NETWORK SECURITY

3.1 Enhance awareness of computer network security prevention

After using the computer, computer users should promptly clear the private information in the computer, encrypt the information in the computer, and prevent personal information from being leaked on public computers. Personal ID information, photos, home addresses, etc. cannot be exposed on the internet at will to prevent inconvenience to oneself. If someone encounters a website that may have problems while surfing the internet, do not click on it casually to prevent viruses from entering the computer system. When using a computer, a firewall should be installed, and vulnerabilities and patches in the system should be regularly checked to reduce the impact of computer viruses and vulnerabilities on computer security.

Government departments and enterprises should cultivate talents in computer network security when preventing computer network security issues, and jointly establish talent training mechanisms with universities to develop efficient network security protection methods, in order to reduce the threats posed by hackers, viruses, and other threats to computer networks. Especially in key units and enterprises, computers contain a large amount of important information and files. When using computers, it is necessary to enhance awareness of network security protection and take effective protective measures to reduce the threat of viruses and other threats to computer systems.

3.2 Installing Computer Security Protection Software

Installing security protection software is an effective measure to ensure the security of computer networks, which can greatly improve the security of computer network systems. Security protection software can effectively prevent viruses from affecting computer network systems as before. Once a network virus invades a computer system, the functions of security protection software will quickly start, filter and intercept network viruses, achieving real-time health and protection of the entire computer network environment. Security protection software can monitor and control virus information in computer network systems. Once a network virus maliciously changes the data in the computer system, the security protection software will pop up as soon as possible, reminding users to pay attention to scanning and killing computer network viruses to ensure the security of computer network data information.

3.3 Timely installation of vulnerability patches

With the continuous development of modern science and technology in our country, computer hardware settings have become increasingly sophisticated.

The types and functions of software are becoming more comprehensive, and computers often receive prompts for installing patches and system updates. If computer users ignore these update prompts, it is difficult to install patches and update the system in a timely manner, which can easily lead to corresponding vulnerabilities in the computer network. To address this issue, computer users can download corresponding virus scanning and security protection software from the official website, among which Rising Antivirus and 360 Security Guard are the most common virus scanning and security protection software. This type of software can ensure the security of the computer system to the greatest extent possible.

3.4 Regularly backup important computer files

Computer users should develop the habit of regularly backing up their computer files, especially important file materials, which should be stored regularly. Hackers and computer virus attacks have strong randomness, and their attack methods, attack times, and other uncertainties are the biggest security threats to computer network systems. Developing the habit of regularly backing up important computer files and minimizing the leakage of critical information is of great significance for maintaining the security and stability of computer network systems.

Computer users backup important files to other hard disk devices and save them, so that even if the computer network is maliciously attacked, there will be no problem of important data loss, effectively ensuring the security of user data information.

3.5 Use of data encryption technology

This technology can encrypt data information in computer networks, minimizing the problem of data theft and tampering, and ensuring the security of data transmission in computer networks. Data encryption technology includes various types, such as plaintext data encryption technology, ciphertext data encryption technology, key data encryption technology, encryption algorithm technology, etc. The most important and critical technology in data encryption is key encryption technology, which can ensure the security and privacy of computer network data information, effectively prevent illegal personnel and malicious software from tampering and stealing data information, and greatly protect the legitimate interests of third-party users. As one of the data encryption technologies, data signature technology can ensure the security of information transmission on the Internet. Data signature technology can effectively prevent external forces from stealing network data information. Digital signature technology can be applied in various stages of data transmission. Users can use secure passwords to protect important computer network data information, ensure the security of data information throughout the entire computer network transmission process, and safeguard the legitimate rights and interests of users.

3.6 Strengthen network system monitoring

In the process of network system operation, various illegal intrusion phenomena occur from time to time. If not detected in a timely manner, it will lay hidden dangers to the security of the network system and cause incalculable losses.

To effectively address some security risks in computer networks, monitoring of network systems is essential. Intrusion detection belongs to comprehensive protection technology, which analyzes and monitors the real-time operation status of the network communication monitoring system to timely detect illegal intrusion phenomena that occur in the network system. In the process of regulating network systems, signature and statistical analysis will be conducted to more effectively address potential security issues and provide protection for network security by monitoring network system vulnerabilities and conducting statistical analysis of network system operation status.

3.7 Strengthen the maintenance of computer hardware facilities

Staff should regularly strengthen the maintenance and upkeep of computer hardware settings to prevent line failures and component damage from hindering the normal operation of the host, and to improve the security and stability of computer networks. Computer users should avoid external interference with the network, and avoid placing their computers in damp and static environments to prevent external factors from interfering with the safe operation of the computer network.

3.8 Network Firewall Settings

Effective application of network firewalls can provide effective protection against malicious attacks from the outside world, as well as constrain the access of internal users to websites with security risks. If the enterprise's internal computer system is connected to the Internet, network security issues need not only to effectively resist viruses, but also to prevent system vulnerabilities. In addition, it is important to pay attention to the prevention of hackers, as network firewalls can take strict preventive measures against malicious intrusions from external networks. On this basis, it is necessary to reasonably divide the internal network of the enterprise and minimize the impact of security issues on the internal network of the enterprise. The setting of firewalls can closely monitor and audit the process of network information transmission and reading, and record all access records in detail. Based on this, corresponding access logs can be generated, which can provide powerful reference for subsequent network security maintenance work. Once there is a network security issue, the firewall can issue an alert in the first time, and also provide the type of problem and related handling suggestions.

4. CONCLUSION

At present, there are mainly system vulnerabilities, computer viruses, and information leaks in computer network systems, which pose a threat to the stability of the system and the security of data information. Therefore, in order to further improve the security of computer networks, it is necessary to enhance users' awareness of security precautions, introduce security protection technologies, strengthen monitoring of network systems, and effectively ensure the security and stability of network systems.

REFERENCES

[1] Liang, X., & Chen, H. (2019, July). A SDN-Based Hierarchical Authentication Mechanism for IPv6 Address. In 2019 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 225-225). IEEE.

[2] Li, L., Gan, Y., Bi, S., & Fu, H. (2024). Substantive or strategic? Unveiling the green innovation effects of pilot policy promoting the integration of technology and finance. International Review of Financial Analysis, 103781.

[3] Wang, Z., Chu, Z. C., Chen, M., Zhang, Y., & Yang, R. (2024). An Asynchronous LLM Architecture for Event Stream Analysis with Cameras. Social Science Journal for Advanced Research, 4(5), 10-17.

[4] Dr, Christopher, Gordon, Ray, & Debus. (2002). Developing deep learning approaches and personal teaching efficacy within a preservice teacher education context. British Journal of Educational Psychology.

[5] Wang, Z., Zhu, Y., Chen, M., Liu, M., & Qin, W. (2024). Llm connection graphs for global feature extraction in point cloud analysis. Applied Science and Biotechnology Journal for Advanced Research, 3(4), 10-16.

[6] Ren, Z. (2024). Enhanced YOLOv8 Infrared Image Object Detection Method with SPD Module. Journal of Theory and Practice in Engineering and Technology, 1(2), 1–7. Retrieved from https://woodyinternational.com/index.php/jtpet/article/view/42

[7] Tian, Q., Wang, Z., Cui, X. Improved Unet brain tumor image segmentation based on GSConv module and ECA attention mechanism. arXiv preprint arXiv:2409.13626.

[8] Ren, Z. (2024). VGCN: An Enhanced Graph Convolutional Network Model for Text Classification. Journal of Industrial Engineering and Applied Science, 2(4), 110-115.

[9] Liang, X., & Chen, H. (2019, July). A SDN-Based Hierarchical Authentication Mechanism for IPv6 Address. In 2019 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 225-225). IEEE.

[10] Shen, Z., Ma, Y., & Shen, J. (2024). A Dynamic Resource Allocation Strategy for Cloud-Native Applications Leveraging Markov Properties. International Journal of Advance in Applied Science Research, 3, 99-107.

[11] Xu, G., Xie, Y., Luo, Y., Yin, Y., Li, Z., & Wei, Z. (2024). Advancing Automated Surveillance: Real-Time Detection of Crown-of-Thorns Starfish via YOLOv5 Deep Learning. Journal of Theory and Practice of Engineering Science, 4(06), 1–10. https://doi.org/10.53469/jtpes.2024.04(06).01

[12] Xu, Y., Gao, W., Wang, Y., Shan , X., & Lin, Y.-S. (2024). Enhancing user experience and trust in advanced LLM-based conversational agents. Computing and Artificial Intelligence, 2(2), 1467. https://doi.org/10.59400/cai.v2i2.1467

[13] Yao, J. (2024). The Impact of Large Interest Rate Differentials between China and the US bn the Role of Chinese Monetary Policy -- Based on Data Model Analysis. Frontiers in Economics and Management, 5(8), 243-251.

[14] Guo, X. , Singh, S. , Lee, H. , Lewis, R. , & Wang, X. . (2014). Deep learning for real-time Atari game play using offline Monte-Carlo tree search planning. International Conference on Neural Information Processing Systems (Vol.4, pp.3338-3346). MIT Press.

[15] Luo, Y., Wei, Z., Xu, G., Li, Z., Xie, Y., & Yin, Y. (2024). Enhancing E-commerce Chatbots with Falcon-7B and 16-bit Full Quantization. Journal of Theory and Practice of Engineering Science, 4(02), 52–57. https://doi.org/10.53469/jtpes.2024.04(02).08

[16] Chen, H., Shen, Z., Wang, Y., & Xu, J. (2024). Threat Detection Driven by Artificial Intelligence: Enhancing Cybersecurity with Machine Learning Algorithms.